What is PHI?

The Health Insurance Portability and Accountability Act, (HIPAA), Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

The HIPAA Security Rule refers specifically to electronic protected health information, (ePHI).

“Individually identifiable health information” is information, including demographic data, that relates to:

- The individual’s past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual, or for which there is a reasonable basis to believe can be used to identify the individual.

Basically, PHI/individually identifiable health information becomes such when the above information is associated with any of the HIPAA common identifiers, listed below. In essence, an individual’s medical history or medical payment history along with any of the common identifiers is considered to be PHI since it could potentially be used to identify the individual and associate him/her with the health care related information. Note, health care information without identifiers is not PHI.

PHI = (Physical or mental health or condition information, or Provision of health care information, or Provision of health care payment information) + (Identifier)

List of 18 Identifiers

1. Names.
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Phone numbers.
5. Fax numbers.
6. Electronic mail addresses.
7. Social Security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger and voice prints.
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo: David.Wargo@uphs.upenn.edu
For more security related information, visit the PMACS Information Security web page:
http://www.med.upenn.edu/pmacs/